UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/783,843	02/15/2001	James Alexander Reeds III	CING-135	2575

39013 7590 10/24/2007

MOAZZAM & ASSOCIATES, LLC
7601 LEWINSVILLE ROAD
SUITE 304
MCLEAN, VA 22102

EXAMINER	
DINH, MINH	

ART UNIT	PAPER NUMBER
2132	

MAIL DATE	DELIVERY MODE
10/24/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	09/783,843	REEDS ET AL.	
	Examiner	Art Unit	
	Minh Dinh	2132	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *16 August 2007*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *37-40* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *37-40* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *15 February 2001* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

Response to Amendment

1. This action is in response to the amendment filed 08/16/2007.

Response to Arguments

2. Applicant's arguments filed 08/16/07 have been fully considered but they are not persuasive.

With respect to the rejection of claims 37-40 under 35 USC 102(e), Applicant argues that Rezaiifar et al. (6,980,658) does not discloses teach or suggest a method for stream cipher out-of-synchronization detection (page 4, 4th paragraph). Rezaiifar discloses an encryption method used in a mobile communication system, i.e., an IS-95 standard system that utilizes stream ciphering (Abstract; fig. 1; col. 1, lines 18-27; col. 3, lines 64-67). Specifically, Rezaiifar discloses a method for a receiving side to detect whether a crypto_synch value is out of synchronization with a crypto_synch value at the transmission side (fig. 10; col. 9, lines 11-30). Rezaiifar also discloses that the "crypto_synch" value is used in ciphering data (col. 4, lines 46-62; lines col. 8, lines 45-50). Rezaiifar further discloses that, by detecting that a crypto_synch value is out of synchronization, the method does detect that the stream cipher is out of synchronization, i.e., detect a failure in decryption (fig. 11, steps 920-930).

Regarding the rejections of claim 37-40 under 35 USC 103(a), Applicant argues that neither Lockhart et al. (5,841,873) nor Menezes et al. ("Handbook of Applied Cryptography") recites a detection method for stream cipher out-of-synchronization detection for validating the integrity of a data packet by comparing a checksum with a calculated checksum to detect the loss of stream cipher synchronization (page 5, 1st full paragraph). Since the rejection is a 103 rejection, it is expected that each reference used in the combination does not disclose all of the limitations. Lockhart does not explicitly disclose the cipher method used is stream cipher. Therefore, Menenzes is relied upon for the teaching of using stream cipher.

Applicant argues that there is no specific motivation disclosed or suggested in the cited prior art to combine the references (page 5, 1st full paragraph). Menezes specifically discloses that stream ciphers are generally faster (than block cipher in hardware), have less complex hardware circuitry, are more appropriate or even mandatory when buffering is limited, and have limited or no error propagation (page 191, Section 6.1 Introduction).

Claim Rejections - 35 USC § 102

3. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

4. Claims 37-40 are rejected under 35 U.S.C. 102(e) as being anticipated by Rezaiifar et al. (6,980,658). Rezaiifar discloses an encryption method used in a mobile communication system, i.e., an IS-95 standard system that utilizes stream ciphering (Abstract; fig. 1; col. 1, lines 18-27; col. 3, lines 64-67).

Regarding claim 37, Rezaiifar discloses a method comprising decrypting a data packet (i.e., a protocol data unit – PDU) containing a Cyclic Redundancy Check (CRC) value, the CRC being functionally equivalent to a checksum, and a payload; extracting the CRC from the decrypted data packet; calculating a CRC for the data packet; comparing the CRC extracted from the decrypted data packet with the calculated CRC; and detecting a loss of stream cipher synchronization if the calculated CRC does not match the CRC extracted from the decrypted data packet, i.e., detecting a failure in decryption (figure 10, elements 810-812; col. 4, lines 46-62; col. 7, lines 15-26, 46-54; col. 8, lines 45-50; col. 9, lines 11-30).

Regarding claims 38-39, Rezaiifar further discloses that the data packet is generated from layer L3 of a protocol stack wherein layer L3

includes TCP/IP layers (figure 2, elements 200, 203). Therefore, layer L3 is a network layer.

Regarding claim 40, Rezaiifar further discloses re-synchronizing a stream cipher if the CRCs do not match (col. 9, lines 23-42).

Claim Rejections - 35 USC § 103

5. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

6. Claims 37-40 are rejected under 35 U.S.C. 103(a) as being unpatentable over Lockhart et al. (5,841,873) in view of Menezes et al. ("Handbook of Applied Cryptography").

Regarding claim 37, Lockhart discloses a method comprising decrypting a data packet containing a checksum and a payload; extracting the checksum from the decrypted data packet; calculating a checksum for the data packet; comparing the checksum extracted from the decrypted data packet with the calculated checksum; and detecting a loss of cipher synchronization if the calculated checksum does not match the checksum extracted from the decrypted data packet (figure 2). Lockhart does not

disclose that the encryption algorithm is a stream cipher. Menezes discloses using stream ciphers (p. 191, see 6.1 Introduction). It would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the method of Lockhart to use a stream cipher, as taught by Menezes, because stream ciphers have limited or no error propagation and, therefore, are advantageous in situations where transmission errors are highly probable (Section 6.1 Introduction, p. 191).

Regarding claims 38-39, Lockhart further discloses that the layer that detects loss of cipher synchronization also handles flow control (i.e., to provide acknowledgement of packet reception) and terminates connection (col. 5, lines 34-45). It is well known that flow control and connection termination are services provided by the transport layer of the protocol stack, which is a network layer.

Regarding claim 40, Lockhart further discloses re-synchronizing the cipher if the checksums do not match (fig. 3).

Conclusion

7. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

Lin et al., "IS-95 North American Standard – A CDMA Based Digital Celluar System"

8. **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Minh Dinh whose telephone number is 571-272-3802. The examiner can normally be reached on Mon-Fri: 10:00am-6:30pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on 571-272-3799. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/MD/
Minh Dinh
Examiner
Art Unit 2132

10/18/07

GILBERTO BARRON JR
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100